IN THE CLAIMS:

1. (Currently amended) An encryption key management system comprising:

a master key;

a portable processor, wherein the portable processor uses the master key for generating an encryption key; [[and]]

a variable key range variable, wherein the portable processor further uses the variable key range variable for generating the encryption key, wherein the variable key range variable comprises at least one of a card number, a card group number and a reference number representing a number of keys; and

an incrementor for increasing the value of the reference number in response to the encryption key being generated.

2. (Canceled)

3. (Previously presented) The encryption key management system recited in claim 1, wherein the variable key range variable is output with the encryption key.

4. (Canceled)

5. (Previously presented) The encryption key management system recited in claim 1, wherein the portable processor further comprises:

a hashing function for generating the encryption key.

6. (Original) The encryption key management system recited in claim 1, wherein the portable processor is a smart card.

7. (Original) The encryption key management system recited in claim 6, wherein the smart card is accessed through verification of a personal identification number.

8. (Canceled)

9. (Original) The encryption key management system recited in claim 1, wherein the portable processor is a first portable processor and the system further comprises:

a second portable processor, wherein the portable processor uses the master key for generating a decryption key.

10. (Original) The encryption key management system recited in claim 9, wherein the second portable processor further uses the variable key range variable for generating the encryption key.

11. (Original) The encryption key management system recited in claim 10, wherein the variable key range variable is input to the second portable processor.

12. (Original) The encryption key management system recited in claim 10, wherein the second portable processor further comprises:

a hashing function for generating the decryption key using the master key.

13. (Original) The encryption key management system recited in claim 9, wherein the second portable processor is a smart card.

14. (Original) The encryption key management system recited in claim 13, wherein the smart card is accessed through verification of a personal identification number.

15. (Original) The encryption key management system recited in claim 10, wherein the second portable processor further comprises:

a hashing function for generating the decryption key.

16. (Currently amended) An encryption key management system comprising:

a master key;

a portable processor, wherein the portable processor uses the master key for generating a decryption key; [[and]]

a variable key range variable, wherein the portable processor further uses the variable key range variable for generating the decryption key, wherein the variable key range variable comprises at least one of a card number, a card group number, and a reference number representing a number of keys; and

an incrementor for increasing the value of the reference number in response to the decryption key being generated.

17. (Canceled)

18. (Previously presented) The encryption key management system recited in claim 16, wherein the variable key range variable is output with the decryption key.

19. (Canceled)

20. (Previously presented) The encryption key management system recited in claim 16, wherein the portable processor further comprises:

a hashing function for generating the decryption key.

21. (Original) The encryption key management system recited in claim 16, wherein the portable processor is a smart card.

22. (Currently amended) An encryption key management method comprising:

receiving a master key;

generating an encryption key using the master key, wherein the encryption key is generated by a portable processor;

outputting the encryption key; [[and]]

creating a variable key range variable, wherein the portable processor uses the variable key range variable for generating the encryption key, wherein the variable key range variable comprises at least one of a card number, a card group number, and a reference number representing a number of keys; and

incrementing an incrementor for increasing the value of the reference number in response to the encryption key being generated.

23. (Canceled)

24. (Previously presented) The method recited in claim 22 further comprises:
outputting the variable key range variable.

25. (Canceled)

26. (Previously presented) The method recited in claim 22, wherein generating the encryption key further comprises:
hashing the master key.

27. (Previously presented) The method recited in claim 22, wherein the portable processor is a smart card.

28. (Original) The method recited in claim 27 further comprises:
verifying a personal identification number; and
accessing functionality of the smart card.

29. (Original) The method recited in claim 22, wherein the portable processor is a first portable processor and the method further comprises:
generating a decryption key using the master key, wherein the decryption key is generated by a second portable processor; and
outputting the decryption key.

30. (Original) The method recited in claim 29, prior to generating the encryption key further comprises:
receiving a variable key range variable, wherein the second portable processor uses the variable key range variable for generating the encryption key.

31. (Previously presented) The method recited in claim 22, wherein the second portable processor is a smart card.

32. (Original) The method recited in claim 22, wherein a smart card is accessed through verification of a personal identification number.

33. (Currently amended) An encryption key management method comprising:

receiving a master key; and

generating a decryption key using the master key, wherein the decryption key is generated by a portable processor;

outputting the decryption key; [[and]]

creating a variable key range variable, wherein the portable processor uses the variable key range variable for generating the decryption key, wherein the variable key range variable comprises at least one of a card number, a card group number, and a reference number representing a number of keys; and

incrementing an incrementor for increasing the value of the reference number in response to the decryption key being generated.

34. (Canceled)

35. (Previously presented) The method recited in claim 33 further comprises:

outputting the variable key range variable.

36. (Canceled)

37. (Previously presented) The method recited in claim 33, wherein generating the decryption key further comprises:

hashing the master key

38. (Previously presented) The method recited in claim 33, wherein the portable processor is a smart card.